

Cloudera Runtime 7.0.2

## Ranger Auditing

Date published: 2019-11-01

Date modified:

# CLOUdera

<https://docs.cloudera.com/>

# Legal Notice

© Cloudera Inc. 2024. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Unless otherwise noted, scripts and sample code are licensed under the Apache License, Version 2.0.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 (“ASLv2”), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER’S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

# Contents

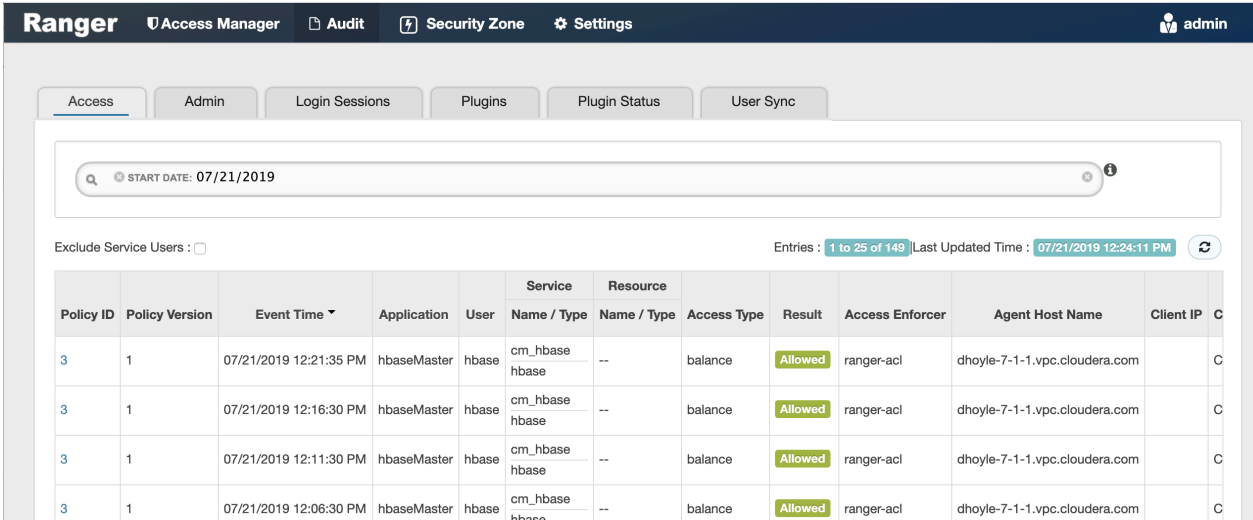
<b>Audit Overview.....</b>	<b>4</b>
<b>Managing Auditing with Ranger.....</b>	<b>4</b>
View audit details.....	4
Create a read-only Admin user (Auditor).....	7

## Audit Overview

Apache Ranger provides a centralized framework for collecting access audit history and reporting data, including filtering on various parameters. Ranger enhances audit information obtained from Hadoop components and provides insights through this centralized reporting capability.

## Managing Auditing with Ranger

To explore options for auditing policies in Ranger, click Audit in the top menu.



The screenshot shows the Ranger web interface. The top navigation bar includes 'Ranger', 'Access Manager', 'Audit', 'Security Zone', and 'Settings'. The user is logged in as 'admin'. Below the navigation bar are tabs for 'Access', 'Admin', 'Login Sessions', 'Plugins', 'Plugin Status', and 'User Sync'. The 'Audit' tab is active, displaying a search bar with 'START DATE: 07/21/2019'. Below the search bar, there is a table of audit entries. The table has columns for Policy ID, Policy Version, Event Time, Application, User, Service Name / Type, Resource Name / Type, Access Type, Result, Access Enforcer, Agent Host Name, Client IP, and a 'C' column. The table shows four entries, all with a result of 'Allowed'.

Policy ID	Policy Version	Event Time	Application	User	Service Name / Type	Resource Name / Type	Access Type	Result	Access Enforcer	Agent Host Name	Client IP	C
3	1	07/21/2019 12:21:35 PM	hbaseMaster	hbase	cm_hbase hbase	--	balance	Allowed	ranger-acl	dhoyle-7-1-1.vpc.cloudera.com		C
3	1	07/21/2019 12:16:30 PM	hbaseMaster	hbase	cm_hbase hbase	--	balance	Allowed	ranger-acl	dhoyle-7-1-1.vpc.cloudera.com		C
3	1	07/21/2019 12:11:30 PM	hbaseMaster	hbase	cm_hbase hbase	--	balance	Allowed	ranger-acl	dhoyle-7-1-1.vpc.cloudera.com		C
3	1	07/21/2019 12:06:30 PM	hbaseMaster	hbase	cm_hbase hbase	--	balance	Allowed	ranger-acl	dhoyle-7-1-1.vpc.cloudera.com		C

There are six tabs on the Audit page:

- Access
- Admin
- Login sessions
- Plugins
- Plugin Status
- User Sync

## View audit details

How to view operation details in Ranger audits.

### Procedure

To view details for a particular operation, click any tab, then Policy ID, Operation name, or Session ID.

Audit > Access: HBase Table

The screenshot shows the Ranger Access Manager interface. The 'Access' tab is selected, and the 'START DATE' is set to 07/21/2019. A table of audit entries is displayed with columns for Policy ID, Policy Version, Event Time, Application, User, Service Name / Type, Resource Name / Type, Access Type, Result, and Access. One entry is highlighted with a blue box, and a 'Policy Details' modal is open over it. The modal shows details for Policy ID 3, Version 1, and lists various resources like 'all - table, column-family, column' with their respective access permissions (Enabled/Include/Exclude).

Policy ID	Policy Version	Event Time	Application	User	Service Name / Type	Resource Name / Type	Access Type	Result	Access
3	1	07/21/2019 12:51:30 PM	hbaseMaster	hbase	cm_hbase hbase	--	balance	Allowed	ranger
3	1	07/21/2019 12:46:30 PM	hbaseMaster	hbase	cm_hbase hbase	--	balance	Allowed	ranger
3	1	07/21/2019 12:41:30 PM	hbaseMaster	hbase	cm_hbase hbase	--	balance	Allowed	ranger-acl
3	1	07/21/2019 12:36:30 PM	hbaseMaster	hbase	cm_hbase hbase	--	balance	Allowed	ranger-acl
3	1	07/21/2019 12:31:31 PM	hbaseMaster	hbase	cm_hbase hbase	--	balance	Allowed	ranger-acl
3	1	07/21/2019 12:26:30 PM	hbaseMaster	hbase	cm_hbase hbase	--	balance	Allowed	ranger-acl

Audit > Admin: Update

The screenshot shows the Ranger Access Manager interface with the 'Admin' tab selected. The 'Search for your access logs...' field is empty. A table of administrative operations is displayed with columns for Operation, Audit Type, User, Date, Actions, and Session Id. One entry is highlighted with a blue box, and an 'Operation: update' modal is open over it. The modal shows details for the 'tag\_service2' operation, including the date and user, and a table of fields with their old and new values.

Operation	Audit Type	User	Date ( Eastern Daylight Time )	Actions	Session Id
Service updated tag_service2	Ranger Service	admin	07/21/2019 01:09:34 PM	Update	40
Group created temp_employees	Ranger Group	admin	07/20/2019 02:15:05 PM	Create	38
Group created audit	Ranger Group	admin	07/18/2019 04:18:42 PM	Create	35
Exported policies	Ranger Policy	admin	07/17/2019 03:06:22 PM	Export, Import	32
Service updated tag_service1	Ranger Service	admin	07/15/2019 04:11:25 PM	Update	
Policy created EXPIRES_ON	Ranger Policy		07/15/2019 04:11:25 PM	Create	
Service created tag_tag	Ranger Service		07/15/2019 04:11:25 PM	Create	
Policy created tag_tag	Ranger Policy		07/15/2019 04:11:25 PM	Create	
Service created tag_tag	Ranger Service		07/15/2019 04:11:25 PM	Create	
Policy created tag_tag	Ranger Policy		07/15/2019 04:11:25 PM	Create	
Service created tag_tag	Ranger Service		07/15/2019 04:11:25 PM	Create	
Policy created tag_tag	Ranger Policy		07/15/2019 04:11:25 PM	Create	
Policy created all - global	Ranger Policy	admin	07/14/2019 05:04:32 PM	Create	27
Policy created all - hivesservice	Ranger Policy	admin	07/14/2019 05:04:32 PM	Create	27
User created auditor1	Ranger User	admin	07/14/2019 05:02:58 PM	Create	27
Service updated em_nfl_registry	Ranger Service		07/11/2019 11:30:39 AM	Update	
Policy created EXPIRES_ON	Ranger Policy		07/11/2019 11:30:39 AM	Create	

Audit > Admin: Create

The screenshot displays the Ranger Admin console interface. At the top, there is a navigation bar with 'Ranger' and menu items: 'Access Manager', 'Audit', 'Security Zone', and 'Settings'. The user 'admin' is logged in. Below the navigation bar, there are tabs for 'Access', 'Admin', 'Login sessions', 'Plugins', 'Plugin status', and 'User sync'. The 'Admin' tab is active, showing a search bar for access logs and a table of audit entries.

The audit log table has the following columns: Operation, Audit Type, User, Date (Eastern Daylight Time), Actions, and Session Id. The entry for 'Security Zone created security-zone2' is highlighted, and a blue arrow points to its 'Create' button in the Actions column.

An 'Operation : create' modal window is open, showing details for the 'security-zone2' operation. The modal includes the following information:

- Name : security-zone2
- Date : 07/14/2019 05:24:36 PM Eastern Daylight Time
- Created By : admin
- Zone Details table:

Fields :	New Value
Zone Description	--
Zone Audit User Groups	--
Zone Audit Users	auditor1
Zone Admin User Groups	--
Zone Admin Users	admin
Zone Tag Services	cm_tag
Zone Name	security-zone2

The modal also includes a 'Zone Service Details' section with fields for 'Service Name' and 'Zone Service Resources', and an 'OK' button at the bottom right.

## Audit > User Sync: Sync details

The screenshot shows the Ranger Admin console interface. At the top, there are navigation tabs: Access, Admin, Login Sessions, Plugins, Plugin Status, and User Sync (selected). Below the tabs is a search bar with the text "START DATE: 07/21/2019". To the right of the search bar, it says "Entries: 1 to 25 of 803" and "Last Updated Time: 07/21/2019 01:23:45 PM".

The main content is a table with the following columns: User Name, Sync Source, Number Of New (Users, Groups), Number Of Modified (Users, Groups), Event Time, and Sync Details. The table contains multiple rows for "rangerusersync" with "Unix" as the sync source. The "Sync Details" column contains eye icons. One eye icon is highlighted with a blue box, and a blue arrow points from it to a modal window titled "Sync Details".

The "Sync Details" modal window shows the following information:

Name	Value
Unix	nss
File Name	/etc/passwd
Sync time	07/21/2019 10:21:48 AM
Last modified time	12/31/1969 04:00:00 PM
Minimum user id	500
Minimum group id	0
Total number of users synced	35
Total number of groups synced	39

An "OK" button is located at the bottom right of the modal window.

## Create a read-only Admin user (Auditor)

Creating a read-only Admin user (Auditor) enables compliance activities because this user can monitor policies and audit events, but cannot make changes.

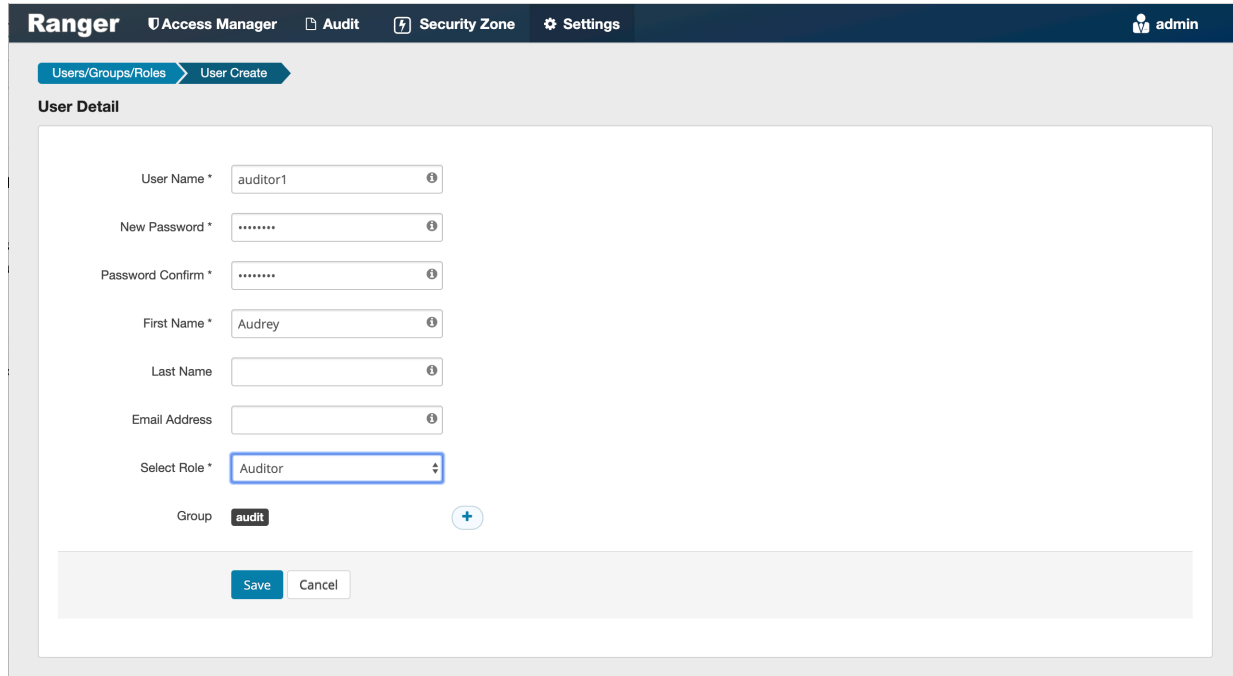
### About this task

When a user with the Auditor role logs in, they see a read-only view of Ranger policies and audit events. An Auditor can search and filter on access audit events, and access and view all tabs under Audit to understand access events. They cannot edit users or groups, export/import policies, or make changes of any kind.

### Procedure

1. Select Settings > Users/Groups/Roles.
2. Click Add New User.

3. Complete the **User Detail** section, selecting Auditor as the role:



The screenshot shows the Ranger web interface for creating a user. The top navigation bar includes 'Ranger', 'Access Manager', 'Audit', 'Security Zone', and 'Settings', with a user profile icon for 'admin'. The breadcrumb trail is 'Users/Groups/Roles > User Create'. The 'User Detail' section contains the following fields:

- User Name \*: auditor1
- New Password \*: [masked]
- Password Confirm \*: [masked]
- First Name \*: Audrey
- Last Name: [empty]
- Email Address: [empty]
- Select Role \*: Auditor (highlighted with a blue border)
- Group: audit (with a plus icon to add more groups)

At the bottom of the form are 'Save' and 'Cancel' buttons.

4. Click Save.